ABSTRACT OF THE DISCLOSURE

The invention relates to a new encrypting device that consists of a CPU core (204) and an encryption algorithm accelerator (205) as main body as well as including a programmable I/O interface (201), a tester and register (202), a reset controller (203), a random number generator (206), a chip ID (207), a security protection unit (208), a shared memory module (209) and an encrypting and decrypting sub-program memory area (210). The invention has solved the shortcomings presented in a single board encrypting system, enhanced the capability against engineering tracking. It meets the strict requirements of the information transmission and information system in the information security area.

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/00

[12]发明专利申请公开说明书

[21]申请号 00117409.6

[43]公开日 2002年3月27日

[11]公开号 CN 1342007A

[22]申请日 2000.9.5 [21]申请号 00117409.6

[71]申请人 深圳市中兴集成电路设计有限责任公司

地址 518058 广东省深圳市南山区麒麟路1号科技创业中心九楼

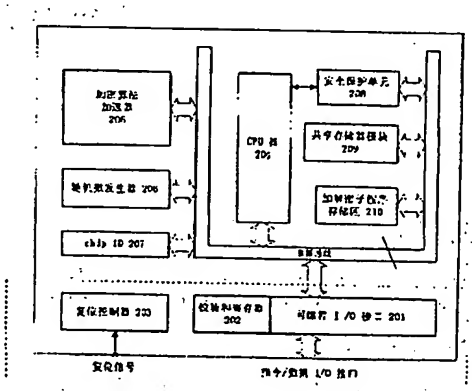
[72]发明人 周玉洁 张苏民

权利要求书1页 说明书6页 附图页数2页

[54]发明名称 一种新的加密装置

[57]摘要

一种新的加密装置，以CPU核(204)与加密算法加速器(205)为主干，包括可编程I/O接口(201)、校验和寄存器(202)、复位控制器(203)、随机数发生器(206)、chipID(207)、安全保护单元(208)、共享存储器模块(209)和加解密子程序存储区(210)；本发明解决了单板加密系统存在的各项不足，提升了装置的抗工程跟踪能力，满足信息安全领域对信息传输与信息系统的严格要求。



ISSN1008-4274

知识产权出版社出版

00.09.19

权 利 要 求 书

1. 一种新的加密装置，其特征在于：包括通过数据总线相连的可编程 I/O 接口（201）、校验和寄存器（202）、复位控制器（203）、CPU 核（204）、加密算法加速器（205）、随机数发生器（206）、chip ID（207）、安全保护单元（208）、共享存储器模块（209）、加解密子程序存储区（210），还包括复位控制器（203）；

所述加密装置通过可编程 I/O 接口（201）与外部系统之间完成数据、指令、地址的交换；

所述可编程 I/O 接口（201）用于所述加密装置与外部系统之间数据、指令、地址的交换；

所述校验和寄存器（202）用于防止消息被篡改和消息误传；

所述复位控制器（203），用于装置的复位以及在特殊情况下外部控制装置的内部信息清除工作；

所述 CPU 核（204）通过增加外围特定辅助电路的方法完善其指令系统，为所述加密装置准备专用的指令集；

所述加密算法加速器（205）用于完成多种密码算法的加解密运算；

所述随机数发生器（206）用于随机数的产生；

所述 chip ID（207）用于存放唯一的装置 ID 号码；

所述安全保护单元（208）执行来自所述复位控制器（203）的强制清除信号指令，根据自身的侦测部件及所述 CPU 核（204）的报警指令，启动自带的应急时钟系统，完成系统自毁。

2. 如权利要求 1 所述的加密装置，其特征在于：所述共享存储器模块（209）由 RAM、EEPROM 组成，分为大小不同的可读写块、只读块、禁读块等块状结构并定义成指令可读写块，用于在密码运算中存放主密钥、私密钥、中间数据等，以及中间结果、内部数据的缓存。

3. 如权利要求 1 所述的加密装置，其特征在于：所述加解密子程序存储区（210）由 RAM、EEPROM 组成，可以存储加密的或非加密的子程序。

4. 如权利要求 1 所述的加密装置，其特征在于：所述 CPU 核（204）可以采用 16 位、32 位、64 位的。

00.09.19

说 明 书

一种新的加密装置

本发明涉及信息安全产品和信息系统安全领域，具体地说，涉及电子商务、Internet 网络、虚拟专用网 VPN 应用等领域中解决信息安全的加密装置。

信息安全、特别是网络环境下的信息安全已成为影响国家安全、经济发展、个人利害、社会稳定的重大问题。从保护国家和个人的利益出发，各国政府无不重视信息和网络安全，特别是各发达国家均大力加强信息安全的研究和督导。最近，美国正在制定新的数据加密标准方案 AES，用以取代 70 年代推出的 DES。各大跨国公司如 IBM、HP、Sun 等均建有强大的信息安全实验室。从我国的国家安全和民族利益出发，不研究网络信息安全问题是不行的，仅仅满足于分散的、以封堵已发现的安全漏洞为目的的研究也不行，而必须从基础着手，对网络环境下的信息安全开展深入的研究，为我国的信息安全提供崭新的、整体的理论指导和基础构件的支撑，并为信息安全技术的实现奠定坚实的基础。

网络环境向信息安全提出了许多新的挑战，在保障信息安全的多种技术手段中，信息加密和密码是保证网络信息安全的重要手段。首先，网络计算为密码分析提供了强有力的工具，使网络环境下的密码学研究、高强度的密码理论、高速的加解密算法、并行密码攻击算法等基础理论的研究取得了很大进展；其次，对网络环境下的用户特征认证、群体数字签名、多方加密算法和多方协议等技术的研究也有了突破。 因此如何保证网络中信息传输的机密性、完整性、有效性和可控性，已成为信息安全领域重要的研究课题。信息的机密性是指信息数据在传输过程中，不能被非授权者偷看；信息的完整性是指信息数据在传输过程中不能被非法篡改；信息的有效性是指信息数据不能被否认；可控性是指合法机构能够对信息及信息系统进行合法监控。采用对称和非对称的密码算法以及衍生算法，加强对密钥管理及采取相关技术措施，可以有效的实现对数据传输可信度的各项要求。

由于信息安全产品的特殊性，信息安全产品直接涉及国家利益、安全和主

权，各国政府对信息产品、信息系统安全性的要求要比对其他产品更为严格。对信息技术和信息安全技术中的核心技术，由政府直接控制，如密码技术和密码产品，多数发达国家都严加控制，即使政府允许出口的密码产品，其关键技术仍控制在政府手中，如美国政府对出口到中国的加密产品的密钥长度加以限制，同时中国政府为了安全考虑也限制使用国外的密码产品，所以必须在国内研制开发自主的密码算法产品。

国内有多家公司推出了一系列的数据加密产品，为用户提供了一系列的客户端和服务器端的安全产品，为电子商务的发展提供了一定的安全保证。数据加密产品作为信息安全产品的一部分，除了有高强抗攻击能力的各种加密算法外，硬件的实现具有重大的意义，良好的硬件设计可以提高整个系统的安全性能。但由于现有硬件条件的限制，所有这类加密产品硬件的实现均是以单板的形式出现，其结构如图 1 所示，所述加密单板包括加密运算协处理器 11、密码程序 12、EEPROM13、随机数发生器 14、安全保护模块 15、随机存储器 RAM16、CPU 控制模块 17 和 I/O 接口 18，各个模块之间通过数据/控制/地址总线相连。

所述加密运算协处理器 11 用于运行密码程序 12，执行数据加密等所需的密码运算，一般用 FPGA 电路装置设计而成。

所述密码程序 12 固化在 ROM 中或写在 EPROM 中，一般以密文的形式存放，当所述加密单板加电后，所述密码程序 12 加载进所述加密运算协处理器 11 中，经解密恢复出明文后再运行。

EEPROM13 用于安全保存主密钥及其它加密运算中所需的安全数据，如 RSA 密钥对等，当所述加密单板加电后，主密钥或 RSA 密钥对由 EEPROM113 调入加密运算协处理器 11 中运算；所述 EEPROM13 还可以根据需要存放所述加密单板的注册类信息。

随机数发生器 14 用于提供生成密钥和管理员、操作员口令所需的随机数，一般使用随机数发生器专用装置。

安全保护模块 15 用于在特殊情况下将所述加密单板上的密码程序 12 和所述 EEPROM13 中的数据擦除或破坏，以防止密钥及加密信息泄露。

随机存储器 RAM16 用于存储运算的中间数据及作为加密单板的其它数据资料的缓存区。

CPU 控制模块 17 用于控制、监控、调度整个加密单板的正常运作，通过 I/O 接口 18 完成单板内部和外部的数据交换，完成所述密码程序 12 的加载工作及适当的辅助工作。

I/O 接口 18 作为加密单板与外部系统的数据和控制通道，一般采用通用的标准接口，如 ISA、PCI 等。

现有加密单板的功能基本上可以满足前面所述的信息传输中对机密性、完整性、有效性的要求，但在实际应用领域中，单板的可控性要求还有不足，由于器件和工艺水平的限制，加密单板缺乏足够的抗工程跟踪能力，其后果是很严重的，整个信息系统的安全将无法保障。下面具体分析存在的隐患：

1. 受单板上器件功能、集成度和规模的限制，单板加密系统必须分模块构成，如图 1 所示，这样各个模块间的寻址、控制和数据信号均要通过相应的总线，而板上的数据总线、控制总线和地址总线均可以被侦测、截取、分析，这样造成了系统安全的隐患。

2. 安全保护模块 15 的作用有限，由于板上各个模块是相互独立的，因此可以采用物理措施隔断安全保护模块 15，使攻击者可以顺利的对其余模块的功能进行分析，而不必担心相关信息的灭失。

3. 由于国内集成电路设计和生产工艺的限制，加密运算协处理器 11 大部分都是用 FPGA 电路实现的，攻击者很容易将其结构破解，分析到加解密算法的电路结构，进而破解固化在 ROM 中的密码程序 12。

4. 密钥的产生及密钥管理在加密机制中占有极其重要的地位，一切加密算法都是围绕着密钥来进行，密钥的泄露将导致整个加密系统的崩溃，后果极其严重，特别是在商用密码领域，由于其大部分的加密算法都是公开的，因此，密钥被破解将会带来巨大的经济损失。加密单板上的 EEPROM13 主要是用来存储密钥的，虽然考虑了密钥的安全管理，但由于前面所述的安全隐患，攻击者可以通过种种手段读取 EEPROM13 中的内容，从而得到密钥，破解加密系统。

5. 单板上的 CPU 控制模块 17 及相应的操作系统，均可能存在“BUG”或是生产商、供应商留有后门，一旦被恶意侵入者利用，就有可能破解整个加密系统，造成巨大的损失。

因此，本发明的目的在于提供一种新的加密装置，可以有效地解决上述安全隐患问题，提高可控性，本发明所述装置将大大提升加密系统的抗工程跟踪能力和系统的安全防护强度。

为达到上述目的，本发明应用片上系统的概念，采用系统集成的方法，提供适应于多种密码算法的加密装置。

本发明所述加密装置包括可编程 I/O 接口、校验和寄存器、复位控制器、CPU 核、加密算法加速器、随机数发生器、chip ID、安全保护单元、共享存储器模块、加解密子程序存储区；除复位控制器外，其他模块相互之间均通过数据总线相连，所述加密装置通过可编程 I/O 接口与外部系统之间完成数据、指令、地址的交换。

下面结合附图，进一步详细说明本发明。

图 1 是现有的加密单板的结构示意图。

图 2 是本发明所述加密装置的结构示意图。

在前面对图 1 已经进行了详细的描述，这里不再赘述。

在图 2 所示的结构图中，断续线将加密装置的内部分为两个区域，线以下部分包括可编程 I/O 接口 201、校验和寄存器 202 及复位控制器 203；所述可编程 I/O 接口 201 用于完成所述加密装置与外部系统之间数据、指令、地址的交换；所述校验和寄存器 202 用于防止消息被篡改和消息误传，是为了增强信息完整性的保障程度而采取的校验方式，类似于一般校验码，但其计算规则不公开，并且不易从一般的校验规则中推导出来；所述复位控制器 203，用于装置的复位以及在特殊情况下外部控制装置的内部信息清除工作，其响应级别是最高的。断续线以下的部分形成了所述加密装置内部和外部系统的隔断。

断续线以上的部分包括 CPU 核 204、加密算法加速器 205、随机数发生器 206、chip ID 207、安全保护单元 208、共享存储器模块 209 和加解密子程序存储区 210，各模块均挂在内部数据总线上，形成了以 CPU 核 204 与加密算法加速器 205 为中心的加密装置主干，CPU 核 204 是整个加密装置的调度指挥中

心。

CPU 核 204 采用 CPU 核技术，可以根据自己的需求，通过增加外围特定辅助电路的方法完善其指令系统，为所述加密装置准备专用的指令集，这些指令集均处于分级保密状态，分别由政府主管部门、应用系统管理员控制；CPU 核 204 可以采用 16 位、32 位、64 位等。

加密算法加速器 205 类似于加密板卡中的加密运算协处理器 11，但其全部采用硬件结构实现相应的加密算法，功能大大强于加密运算协处理器 11。加密算法加速器 205 内部采用模块化结构，完成多种密码算法的加解密运算，其支持的密码算法有：公钥算法，如模长为 512、768、1024、2048、4096 比特的 RSA 算法、模长为 512、1024 比特的 DSA 数字签名算法和椭圆曲线密码算法等；对称算法，如 DES 算法、Triple-DES 算法、RC2 算法、RC4 算法和 IDEA 等对称密钥密码算法；HASH 算法，如 MD2 算法、MD5 算法和 SHA1 算法。

随机数发生器 206 用于随机数的产生，随机数发生器 206 生成的随机数组经过 CPU 核 204 内部处理后产生所需的随机数、密钥或密钥对等数据。

CHIP ID 207 是为了加强装置的可控性，在装置中设置的只能由政府主管部门读/写的区域，其中存放唯一的装置 ID 号码，为主管部门的监察工作提供方便。

安全保护单元 208 执行系统复位控制器 203 的强制清除信号的指令，还可根据自身的侦测部件及 CPU 核 204 的报警指令，启动自带的应急时钟系统，在毫秒级的时间内完成系统自毁，保障系统的信息不被泄露。安全保护单元 208 由于是集成在系统内部，有比单板加密系统中同类单元更强的功能，对系统信息的保护更加可靠。

共享存储器模块 209 由 RAM、EEPROM 组成，分为大小不同的块状结构，分别根据用途定义成指令可读写块、一般可读写块、只读块、禁读块等，用于在密码运算中存放主密钥、私密钥、中间数据等，以及用于 CPU 核 204、加密算法加速器 205 在进行内部运算和加解密处理时的中间结果、内部数据的缓存等用途。

加解密子程序存储区 210 由 RAM、EEPROM 组成，加解密子程序可根据 CPU 核 204 的指令通过可编程 I/O 接口 201 下载，该子程序可以是加密的也可以是

非加密的，该存储区 210 可以通过专用指令设置对外界开放，供使用者测试。

在外部应用系统看来，本发明所述加密装置是一个挂在外部总线上的智能接口单元，外部应用系统可通过片选信号选中此加密装置，并通过片选端、R/W 端及其它控制端的端信号组合通知送到加密装置接口总线的数据的性质。加密装置上电后，自动将校验和寄存器 202 等单元复位，等待初始化进程；CPU 核 204 首先读入接口总线的指令数据，并根据指令到指定区域下载相应的加解密程序及其它加解密算法所需的数据资料、启动随机数发生器 206 生成所需的随机数或密钥等，完成装置其它单元的初始化工作，加密装置转入等待状态，准备进行相关的算法操作；本发明所述装置依据相关程序与外部系统配合进行两种内部操作：加解密数据的输入/输出操作，状态标志为 READY；和内部加解密运算操作，状态标志为 BUSY，这两种状态标志用于通知外部应用系统，以保证装置的可靠运行。

本发明以 CPU 核 204 与加密算法加速器 205 为主干，丰富的 RISC 指令集和强大的数据吞吐能力，提升了整个装置的运算和控制能力，也为实施多种加解密运算必需的专用指令集提供了广阔的选择余地。装置内数据流通过 CPU 核 204 与内部数据总线调度，装置内部与外部的全部数据（包括数据、地址、指令）交流，均通过由 CPU 核 204 控制的可编程 I/O 接口 201 进行，这样把加解密的处理过程有效的与外部隔离。内部 CPU 核 204 通过可编程 I/O 接口 201 从外界读取指令、地址、数据等，均表现为对 I/O 接口的读写操作，而用于加解密运算操作的专用指令也是非公开的，因此，恶意侵入者将难以理解和分析装置 I/O 接口的数据性质，也难以通过对公开指令的操作寻址装置的保密区域，获得有用的资料，这些控制措施都大大提升了装置的抗工程跟踪能力，满足信息安全领域对信息传输与信息系统机密性、完整性、有效性和可控性的严格要求。

综上所述，本发明所述加密装置，解决了单板加密系统存在的各项不足，并可以集成在远小于单板的芯片上，体积大大缩小，更好地满足了信息安全系统中对信息传输的机密性、完整性、有效性和可控性的要求。

00.09.19

说 明 书 附 图

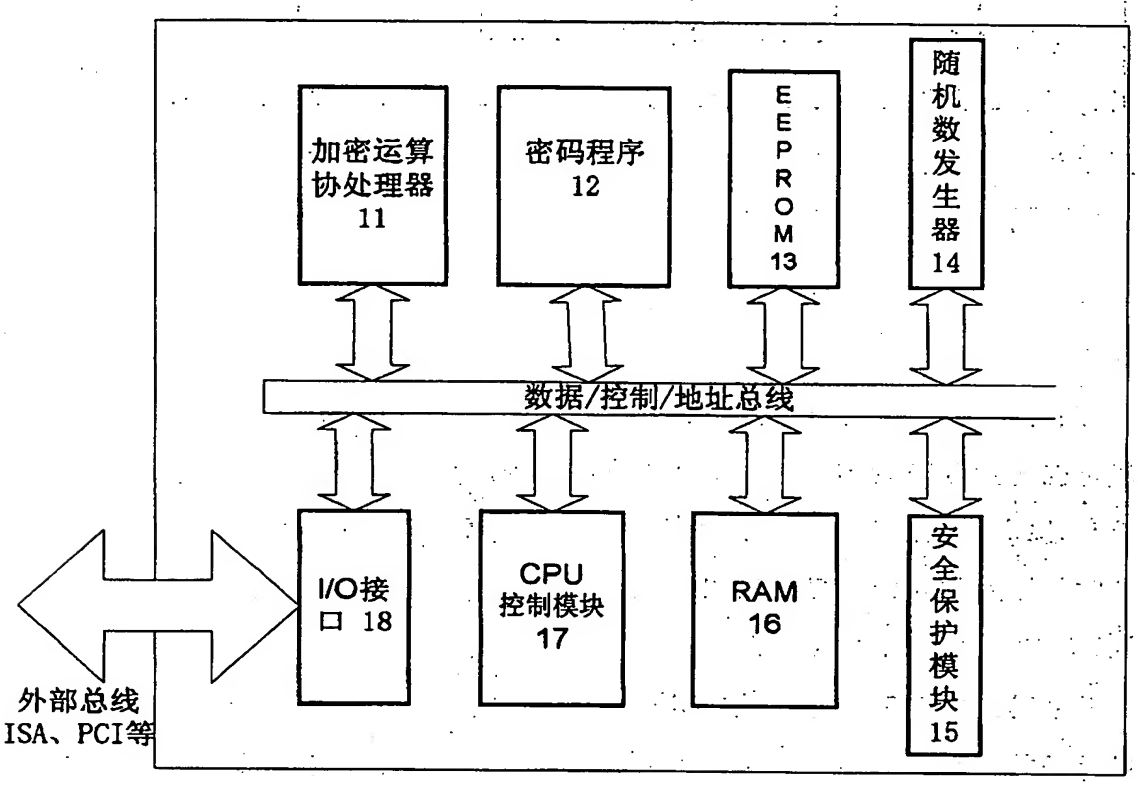


图 1

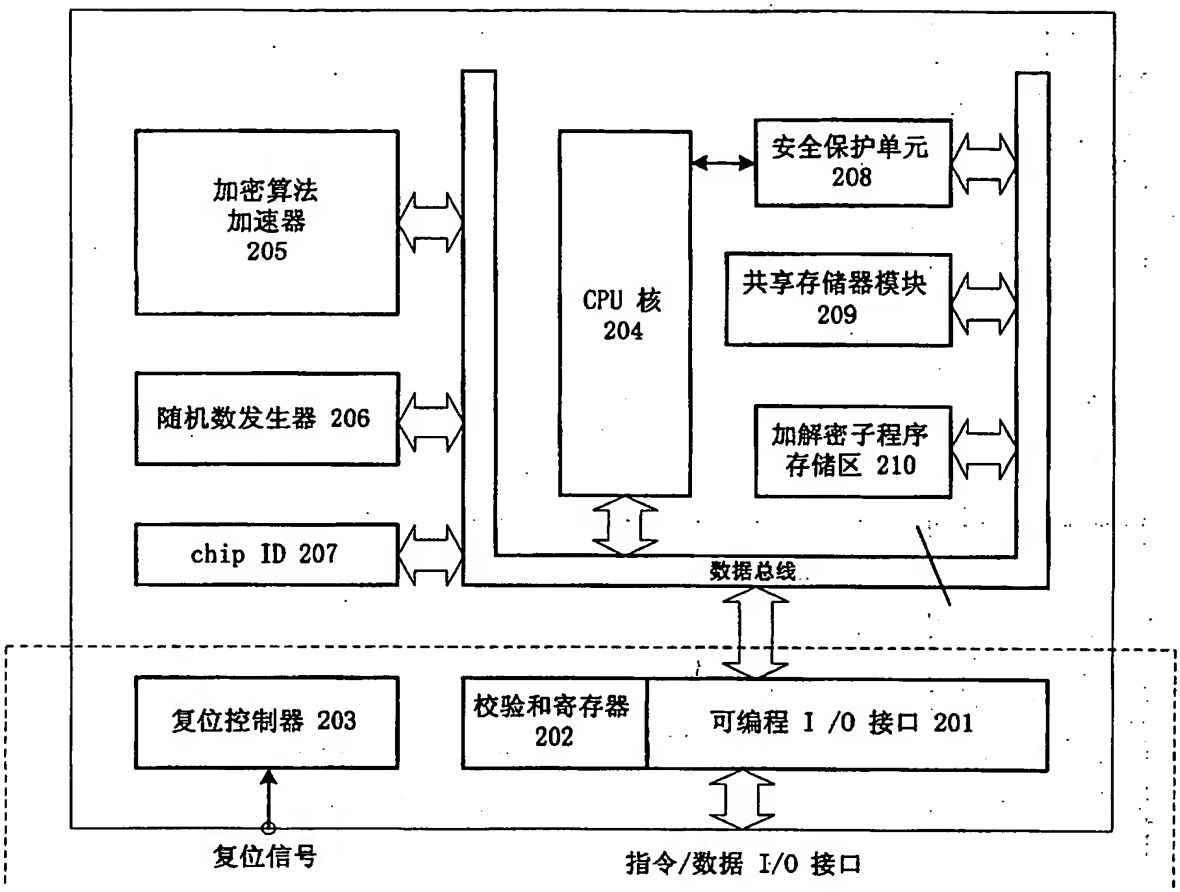

加密算法
加速器
205
随机数发生器 206
chip ID 207
CPU 核
204
安全保护单元
208
共享存储器模块
209
加解密子程序
存储区 210
数据总线
复位控制器 203
校验和寄存器
202
可编程 I /O 接口 201
复位信号
指令/数据 I/O 接口

图 2